UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/660,413	09/10/2003	Alexey Kobozev	50325-0815	5822

29989 7590 06/27/2008

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
BESROUR, SAOUSSEN	
ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
06/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/660,413	KOBOZEV ET AL.	
	Examiner	Art Unit	
	SAOUSSEN BESROUR	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on May 6, 2008 has been entered.

Claims 1-47 are currently being considered.

Response to Arguments

Applicant's arguments filed May 6, 2008 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the Applicant argues that the Cited Prior Art (CPA) does not teach the new limitation of "without parsing or interpreting any data structure in the first security certificate or the second security certificate." The Applicant points to paragraph 0102 for support for this limitation. However, the specification just states that the system "does not necessarily need to know how to parse or interpret the data structure." This is not seen as equivalent to the claim limitation. Therefore, the limitation is not seen as given support. The Applicant is requested to provide a better explanation of how the limitation is supported in the specification. Furthermore, the limitation is seen

as indefinite as it is not clear what function can performed without parsing or interpreting any data structures.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-47 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The limitation is seen as indefinite as it is not clear what function can performed without parsing or interpreting any data structures.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1-41 and 43-47** are rejected under 35 U.S.C. 103(a) as being unpatentable over Silva et al. (US 6,615,347) in view of England et al. (20070174921).

As per **claim 1** de Silva discloses: receiving a first security certificate associated with the sender and storing the first security certificate in a location accessible to the receiver (Column 3, Lines 58-Column 4, Lines 10); updating the first security certificate when the location accessible to the receiver if the first security certificate is changed or revoked (Column 6, Lines 10-34); receiving a second security certificate from the sender when identity of the sender needs to be verified (Column 6, Lines 35-40). De Silva does not explicitly teach: comparing in memory a binary representation of the entire second security certificate to a binary representation of the entire first security certificate; and confirming the sender's identity only when the binary representation of the second security certificate matches the binary representation of the first security certificate for the sender. However, England et al. discloses: comparing in memory a binary representation of the entire second security certificate to a binary representation of the entire first security certificate (0158); and confirming the sender's identity only when the binary representation of the second security certificate matches the binary representation of the first security certificate for the sender (0158). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of England in conjunction with the teachings of De Silva for the benefit of trusted application upgrade (0039)

As per **claim 18** de Silva discloses: copying a first security certificate associated with the client to a location accessible to the server (Column 3, Lines 58-Column 4, Lines 10); updating the first security certificate in the location accessible to the server when the first certificate is changed or revoked (Column 7, Lines 6-30); receiving a

second security certificate from the client when identity of the client needs to be verified (Column 6, Lines 35-40). De Silva does not explicitly teach: comparing in memory a binary representation of the entire second security certificate to a binary representation of the entire first security certificate without parsing of data fields contained within either the first or second security certificate; and confirming the sender's identity only when the binary representation of the second security certificate matches the binary representation of the first security certificate for the sender. However, England et al. discloses: comparing in memory a binary representation of the entire second security certificate to a binary representation of the entire first security certificate without parsing of data fields contained within either the first or second security certificate (0158); and confirming the sender's identity only when the binary representation of the second security certificate matches the binary representation of the first security certificate for the sender (0158). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of England in conjunction with the teachings of De Silva for the benefit of trusted application upgrade (0039)

As per **claim 32** de Silva discloses: receiving a first security certificate associated with the server and storing the first security certificate in a location accessible to the client (Column 3, Lines 58-Column 4, Lines 10); updating the first security certificate in the location accessible to the client when the first security certificate is changed or revoked (Column 7, Lines 6-30); receiving a second security certificate from the server when identity of the server needs to be verified (Column 6, Lines 35-40). De Silva does

not explicitly teach: comparing in memory a binary representation of the entire second security certificate to a binary representation of the entire first security certificate without parsing of data fields contained within either the first or second security certificate; and confirming the sender's identity only when the binary representation of the second security certificate matches the binary representation of the first security certificate for the sender. However, England et al. discloses: comparing in memory a binary representation of the entire second security certificate to a binary representation of the entire first security certificate without parsing of data fields contained within either the first or second security certificate (0158); and confirming the sender's identity only when the binary representation of the second security certificate matches the binary representation of the first security certificate for the sender (0158). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of England in conjunction with the teachings of De Silva for the benefit of trusted application upgrade (0039)

As per **claim 44**, de Silva discloses: receiving a first security certificate associated with the sender and storing the first security certificate in a location accessible to the receiver (Column 3, Lines 58-Column 4, Lines 10); updating the first security certificate when the location accessible to the receiver if the first security certificate is changed or revoked (Column 6, Lines 10-34); receiving a second security certificate from the sender when identity of the sender needs to be verified (Column 6, Lines 35-40). De Silva does not explicitly teach: comparing in memory a binary representation of the entire second security certificate to a binary representation of the

entire first security certificate; and confirming the sender's identity only when the binary representation of the second security certificate matches the binary representation of the first security certificate for the sender. However, England et al. discloses: comparing in memory a binary representation of the entire second security certificate to a binary representation of the entire first security certificate (0158); and confirming the sender's identity only when the binary representation of the second security certificate matches the binary representation of the first security certificate for the sender (0158). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of England in conjunction with the teachings of De Silva for the benefit of trusted application upgrade (0039)

As per **claim 45**, de Silva discloses: receiving a first security certificate associated with the sender and storing the first security certificate in a location accessible to a receiver (Column 3, Lines 58-Column 4, Lines 10); updating the first security certificate in the location accessible to the receiver when the first security certificate is changed or revoked (Column 7, Lines 6-30); receiving a second security certificate from the sender when identity of the sender needs to be verified (Column 6, Lines 35-40 De Silva does not explicitly teach: comparing in memory a binary representation of the entire second security certificate to a binary representation of the entire first security certificate; and confirming the sender's identity only when the binary representation of the second security certificate matches the binary representation of the first security certificate for the sender. However, England et al. discloses: comparing in memory a binary representation of the entire second security certificate to

a binary representation of the entire first security certificate (0158); and confirming the sender's identity only when the binary representation of the second security certificate matches the binary representation of the first security certificate for the sender (0158). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of England in conjunction with the teachings of De Silva for the benefit of trusted application upgrade (0039)

As per **claim 2, 19 and 33**, rejected as applied to claim 1, 18 and 32. Furthermore de Silva discloses: removing the first certificate from the location accessible to the receiver when the first certificate is revoked (Column 7, Lines 6-30); and replacing the first certificate in the location accessible to the receiver if the first certificate is changed (Column 7, Lines 61-63).

As per **claim 3, 20 and 34**, rejected as applied to claims 2, 19 and 33. Furthermore, de Silva discloses: the removing step is performed when the first certificate is known to have been revoked for a reason selected from the group consisting of expiration of the certificate, change of certificate authority, and compromise of the certificate (Column 5, Lines 25-32).

As per **claims 4, 21 and 35**, rejected as applied to claims 2, 19 and 33. Furthermore, de Silva discloses: wherein the replacing step is performed when the first certificate is known to have been changed for a reason selected from the group consisting of expiration of the certificate, change of certificate authority, and compromise of the certificate (Column 5, Lines 25-32).

As per **claim 5**, rejected as applied to claim 1. Furthermore, de Silva discloses: storing the first security certificate in a directory service (Column 3, Lines 51-55).

As per **claim 6 and 22**, rejected as applied to claims 5 and 18. Furthermore, de Silva discloses: wherein the directory service is a Lightweight Directory Access Protocol directory (Column 3, lines 51-55).

As per **claims 7 and 23**, rejected as applied to claims 1 and 18. Furthermore, de Silva discloses: wherein the first certificate is known to have been granted by a certificate authority (Column 3, Lines 50-51).

As per **claims 8 and 24**, rejected as applied to claims 1 and 18. Furthermore, de Silva discloses: wherein the first certificate is known to have been obtained in a trusted domain (Column 3, Lines 50-51).

As per **claim 9, 26 and 36**, rejected as applied to claims 1, 18 and 32. Furthermore, de Silva discloses: herein the step of comparing the first certificate and second certificate comprises comparing a computer memory representation of each certificate (Column 9, Lines 10-25).

As per **claim 10**, rejected as applied to claim 1. Furthermore, de Silva discloses: wherein the sender is a client and the receiver is a server (Column 4, Lines 33-51).

As per **claims 11, 25 and 37**, rejected as applied to claims 10, 18 and 32. Furthermore, de Silva discloses: herein the receiver is an authentication, authorization, and accounting server (Column 4, Lines 33-51).

As per **claim 12**, rejected as applied to claim 1. Furthermore de Silva discloses: wherein the sender is a server and the receiver is a client (Column 4, Lines 33-51).

As per **claim 13, 27 and 38**, rejected as applied to claims 1, 18 and 32. Furthermore, de Silva discloses: wherein the communication between the sender and receiver is in a protocol that requires the inclusion of a digital certificate (Column 4, Lines 55-65).

As per **claims 14, 28 and 39**, rejected as applied to claims 13, 27 and 28. Furthermore, de Silva discloses: wherein the protocol is selected from the group consisting of the Extensible Authentication Protocol and Transport Level Security protocol, the Protected Extensible Authentication Protocol, and the Tunneled Transport Level Security protocol (Column 4, Lines 55-65).

As per **claims 15, 29 and 40**, rejected as applied to claims 1, 18 and 32. Furthermore, de Silva discloses: the second certificate is known to have been signed by a certificate authority (Column 3, Lines 50-51 and Column 1, Lines 40-55, Column 2, Lines 13-26).

As per **claims 16, 30 and 41**, rejected as applied to claims 15, 29 and 40. Furthermore, de Silva discloses: decrypting the second certificate using a public key associated with the certificate authority, whereby the receiver verifies that the certificate authority has signed the second certificate (Column 1, Lines 52-60).

As per **claims 17, 31 and 43**, rejected as applied to claims 1, 18 and 43. Furthermore, de Silva discloses: receiving a message encrypted with the sender's private key; and decrypting the message using the sender's public key (Column 3, Lines 35-50).

As per **claim 46**, rejected as applied to claim 45. Furthermore, England et al. discloses: comparing an occupied length in memory of the first security certificate to an occupied length in memory of the second security certificate before the confirming of the sender' s identity (0158).

As per **claim 47**, rejected as applied to claim 45. Furthermore, England et al. discloses: comparing is performed without parsing of data fields contained within either the first or second security certificates (0158).

7. **Claim 42** is rejected under 35 U.S.C. 103(a) as being unpatentable over de Silva et al. (US 6,615,347) in view of England et al. (20070174921) in further view of Fe et a. (US 20030037234).

As per **claim 42**, rejected as applied to claim 32. The combined references De Silva and England et al. do not explicitly teach wherein the server is one of a plurality of load balanced servers and each server of the plurality of load balanced servers has an identical security certificate, whereby the client need not know to which of the plurality of servers it is attached. However, Fu et al. discloses: wherein the server is one of a plurality of load balanced servers and each server of the plurality of load balanced servers has an identical security certificate, whereby the client need not know to which of the plurality of servers it is attached (0046). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings

of Fu et al. in conjunction with the combined teachings of De Silva and England et al. for the benefit of greater scalability (0012).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SAOUSSEN BESROUR whose telephone number is (571)272-6547. The examiner can normally be reached on M-F 8:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. B./
Examiner, Art Unit 2131

/Kaveh Abrishamkar/
Primary Examiner, Art Unit 2131